Abstract

A system for detecting network intrusions and other conditions in a network is described. The system includes a plurality of collector devices that are disposed to collect data and statistical information on packets that are sent between nodes on a network. An aggregator device is disposed to receive data and statistical information from the plurality of collector devices. The aggregator device produces a connection table that maps each node on the network to a record that stores information about traffic to or from the node. The aggregator runs processes that determine network events from aggregating of anomalies into network events.

20748971.doc